FACHBEITRAG

MODERN AUTHENTICATION (OAUTH 2.0)

446 PLATTFORM® VERSION 2020
STAND: 08.2021

ISONET
25 Jahre
BEE DIGITAL

MODERN AUTHENTICATION

«Modern Authentication» ist ein Überbegriff für verschiedene Authentifizierungsformen. Dazu gehört die Mehrfaktorauthentifizierung, durch die geprüft wird, ob sich die Person, welche sich an einem Konto anmeldet, auch dazu berechtigt ist. Dafür wird zusätzlich zu dem Nutzernamen und Passwort eine weitere Identitäts-Bestätigung, etwa durch die Authenticator-App, benötigt. Ein weiterer zentraler Aspekt ist die Autorisierung von Drittanbieter-Services für spezifische Aufgaben bzgl. eines bestimmten Kontos, also die Regelung, wer in welchem Umfang auf wessen Daten wie zugreifen darf. Die autorisierte Applikation greift im Namen desjenigen, der sie autorisiert hat, auf dessen Ressourcen zu, ohne die eigentlichen Zugangsdaten (Nutzername / Passwort) der Ressource zu kennen. Durch diese Autorisierungen mit OAuth 2.0 wird das Zusammenspiel vernetzter Systeme geregelt.

Die Autorisierung vernetzter Applikationen mit OAuth 2.0 werden wir hier kurz erklären:

Beispiel OAuth 2.0 - Anmeldung der 446 Plattform® Mail2Ticket-Schnittstelle:

Mit der Mail2Ticket-Schnittstelle sollen alle Emails des Microsoft Exchange Postfaches der Emailadresse beehappy@446.world regelmässig abgeholt und in Tickets umgewandelt werden, die einem entsprechenden Mail2Ticket-Workflow folgen. Der Client bzw. Drittanbieter (die 446 Plattform®) soll dafür Daten (Emails) aus dem Resource Server (Postfach «beehappy@446.world») abholen, um konkrete Aufgabe auszuführen (Emails in Tickets umwandeln). Bei diesem indirekten Autorisierungstyp ist der Resource Owner (Besitzer des Mailpostfaches «beehappy@446.world») ein im Azure-AD hinterlegtes Dienstkonto. Die Abbildung 1 zeigt schematisch die Anmeldung und den Aufbau einer sicheren Daten-Verbindung zwischen der 446 Plattform® und dem entsprechenden Microsoft Exchange mit OAuth 2.0. Dabei beschreiben wir die beteiligten Systeme und den Ablauf der Autorisierung:

Beteiligte Systeme

CLIENT:

Die Applikation oder Webseite, die auf eine bestimmte Ressource zugreifen möchte, z.B. der Mail2Ticket Dienst der 446 Plattform®, die auf die Emails in einem bestimmten Postfach auf einem Microsoft Exchange Server zugreifen möchte. Dessen Client wird häufig als Drittanbieter bezeichnet, der selbst keine direkten Zugangsdaten des Resource Owners erhält bzw. kennt.

RESOURCE OWNER:

Der Besitzer der Zugangsinformationen, die der Client benötigt. In diesem Beispiel der Besitzer des Kontos «beehappy@446.world» mit den Zugangsdaten zum Resource Server, auf dem die vom Client benötigten Informationen liegen.

AUTHORIZATION SERVER:

Das System, auf dem die Kontoinformationen des Resource Owners hinterlegt und verifiziert werden, in diesem Beispiel ein Microsoft Azure AD.

RESOURCE SERVER:

Der Server bzw. Ort, an dem die Resourcen, die vom Client benötigten Informationen, gespeichert sind. In diesem Beispiel ein Microsoft Exchange Server.

1. **Autorisierungsanfrage:**

   Im Auftrag des Anwenders fragt der Client (die Mail-Schnittstelle der 446 Plattform®) nach der Erlaubnis des Resource Owners (Postfach Inhaber), um dessen Ressource (Postfach), die auf dem Resource Server (Microsoft Exchange) gehostet ist, zu benutzen. Dies erfolgt bei Service-Konten indirekt (implizites Recht) über den Authorization Server (Authorization Request = „Darf ich in deinem Namen xy tun?“).

2. **Autorisierungsgenehmigung I:**

   Der Client erhält vom Resource Owner eine Autorisierungsgenehmigung. Der Authorization Server verifiziert den Client und kontaktiert den Resource Owner, damit dieser sich authentifiziert (in unserem Beispiel das Service Konto), indem er sich am Resource Server (Microsoft Exchange) stellvertretend mit dem Servicekonto am Postfach einloggt.

3. **Autorisierungsgenehmigung II:**

   Nach der erfolgreichen Authentifizierung wird die Erlaubnis erteilt, dass der Client auf diese Ressource zugreifen darf, da er nun autorisiert und am Postfach authentifiziert ist. Nach erfolgter Genehmigung durch den Resource Owner (Microsoft Exchange Postfach) fordert der Client einen Access Token vom Authorization Server an.

4. **Access Token I:**

   Ist dies erfolgreich, sendet der Authorization Server dem Client einen Access Token.

5. **Access Token II:**

   Nach erfolgreicher Prüfung des Access Tokens (statt Username und Passwort) durch den Resource Server wird eine Direktverbindung zwischen Client und Resource Server aufgebaut.

6. **Geschützter Datentransfer:**

   Die Daten werden vom Resource Server zur Verfügung gestellt, solange der Token gültig ist.

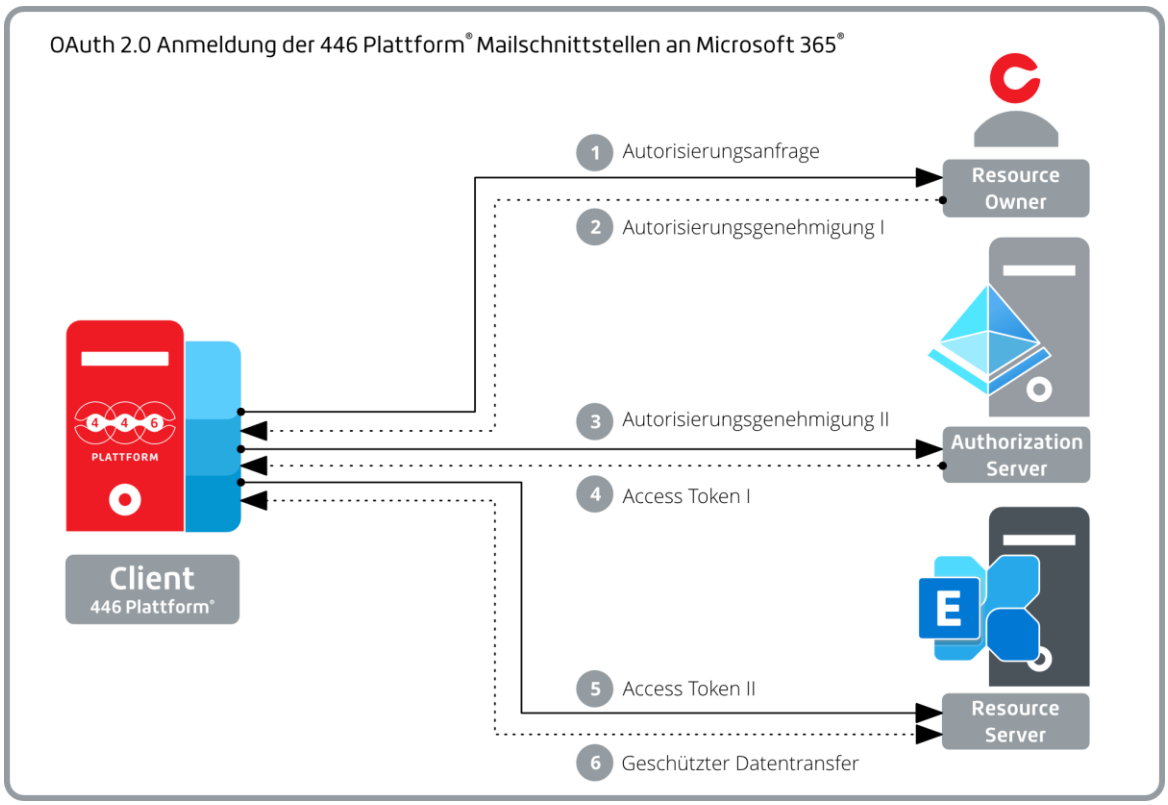

Abb.1: Schematische Darstellung einer OAuth 2.0 - Anmeldung

ÜBER ISONET

Isonet verbindet mit ihrem Systemischen Prozessmanagement, der 446 Methode®, auf innovative Art Prozess-analyse und Unternehmensberatung und befähigt somit Unternehmen, auch die zukünftigen Aufgaben zu lösen. Seit dem Gründungsjahr 1994 betreut das Unternehmen mit seinen Niederlassungen in Zürich (Sitz) und Leipzig zahlreiche Kunden aus verschiedenen Branchen mit unterschiedlichen Unternehmensgrössen. Ziel ist dabei immer die nachhaltige Optimierung von Prozessen und Abläufen, so dass Unternehmen jederzeit agil auf Marktentwicklungen reagieren können. Mit der IT-Lösung der Isonet, der 446 Plattform®, optimieren Sie Ihre Prozesse individuell, flexibel und ganzheitlich.

Gold Microsoft Partner

METHODE PLATTFORM